DEPARTMENT OF THE NAVY
COMMANDER
NAVAL NETWORK WARFARE COMMAND
2465 GUADALCANAL RD
NORFOLK, VA 23521-3228

5239
Ser ODAA/5962
SEP 25 2009

From: Commander, Naval Network Warfare Command
To: Commander, Navy Installations Command

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED COMMON ACCESS CARD (CAC) PIN RESET (CPR) WORKSTATION VERSION 2.1 ON ALL NAVY NETWORKS (FY09J0041) DADMS 49101

Ref: (a) OPNAV Instruction 5239.1C, Navy Information Assurance (IA) Program of 20 Aug 08
(b) DON CIO Washington DC 311917Z Mar 08 Department of the Navy's Transition Plan from DITSCAP to DIACAP
(c) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) of 28 Nov 07
(d) CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities of 9 Jul 08
(e) CJCSM 6510.01 CH-3, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND) of 25 Mar 03
(f) COMNAVNETWARCOM Norfolk VA 211600Z Dec 06 Navy Telecommunications Directive (NTD) 11-06, Promulgation of the System Identification Profile (SIP) for Navy IT Certification and Accreditation Process
(g) COMNAVNETWARCOM Norfolk VA 022152Z May 08 Announcement of the Sustainability and Supportability Document
(h) DoD Instruction 8500.2 Information Assurance (IA) Implementation of 6 Feb 03
(i) NAVCYBERDEFOPSCOM Norfolk VA 062305Z Mar 06 NCDOC Computer Tasking Order (CTO) 06-02 Directive for Automated Scanning and Remediation of Network Vulnerabilities
(j) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management of 15 Aug 04
(k) DoD 8570.01-M, Information Assurance Workforce Improvement Program of 19 Dec 05

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED COMMON ACCESS CARD (CAC) PIN RESET (CPR) WORKSTATION VERSION 2.1 ON ALL NAVY NETWORKS (FY09J0041) DADMS 49101

(l) OPNAV Navy-Marine Corps Unclassified Trusted Network Protection (UTNProtect) Policy, Ver 1.0 of 31 Oct 02 w/changes

(m) DoD CIO Memo, Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media of 3 Jul 07

(n) DON CIO Washington DC 081605Z Jan 09 DON Federal Information Security Management Act Goals for FY 2009

(o) DON CIO Washington DC 181430Z May 09 Department of the Navy Privacy Impact Assessment (PIA) Guidance

(p) CNO Washington DC 180128Z Nov 05 Restrictions on Applications Allowed to Transition into NMCI and or ONE-NET

(q) DON CIO Washington DC 291600Z Feb 08 DON Contingency Plans and Testing Guidance

(r) COMNAVNETWARCOM Norfolk VA 231444Z Aug 07 CARS TF FRAGO 002 - NMCI Transition

(s) COMNAVNETWARCOM ltr 5239 Ser ODAA/1705, Navy ODAA Guidance Memorandum 02-07; Guidance for a Comprehensive Plan of Action and Milestones (POA&M) of 14 Jun 07

(t) Department of Defense (DoD) Memorandum for DoD Information System Certification and Accreditation Reciprocity of 23 Jul 09

(u) Defense Manpower Data Center Memorandum for CPR-WS Users of 7 Aug 06

(v) Information Assurance Tracking System (IATS) website https://iats.nmci.navy.mil, Reference # 11288

1. By authority granted in reference (a), an ATO is hereby granted for the operation of the unclassified CPR version 2.1 on all Navy networks. This ATO serves as a Type Accreditation for Navy networks and requires installation and management per the approved configuration along with site installation Certification and Accreditation (C&A) documentation updates, and is granted in accordance with references (b) and (c), in compliance with references (d) through (u), and based on review of the information contained in reference (v). **The Navy ODAA acknowledges DMDC is responsible for controlling all aspects of the system and they are responsible for accepting the risk provided in reference (u). All local Navy commands using CPR will have to ensure they provide physical/environment security and enclave boundary protection.**

2. This ATO expires on **16 August 2012** or sooner if there are modifications that change the security posture of CPR. Changes must be submitted in writing through the Echelon II representative for Certification and Accreditation processing prior to implementation.

3. The CPR system is composed of four components that provide the capability to reset a locked CAC and change a CAC's PIN. The CPR system uses DEERS to authenticate users and to reset PIN's for established customer. Two CACs and a positive fingerprint identification of the customer are required during the PIN reset process. To capture the appropriate data from these sources, each system on which the CPR application is installed is equipped with two CAC smart readers and a fingerprint scan physically attached to the system.

4. The CPR system has been designated as Mission Assurance Category (MAC) Level II, and is authorized to process information at a confidentiality level of sensitive up to Unclassified in the System High mode of operation.

5. Reference (j) establishes policy to implement Information Assurance (IA) training, certification and workforce management programs for all DoD Component personnel. You are required to take appropriate action, in accordance with references (j) and (k), to ensure the identification and categorization of positions conducting IA functions. This includes ensuring that these individuals are trained and certified in order to professionalize personnel commensurate with their Information System (IS) user responsibilities and IA functions, and to document and track IA awareness training and certification status. IA training and certification requirements also apply to authorized contractor users and contractor personnel performing IA functions.

6. Based upon review of available documentation, the NNWC Action Officer assessed the overall risk of **Medium**. In order to retain this ATO, you are required to comply with all DoD and Navy policy requirements for IA and ensure the items listed below are accomplished. Non-compliance may result in termination of this ATO. Solutions for correcting technical issues must be submitted in writing to the Navy CA for review and forwarded to the Navy ODAA for approval. For non-technical issues, written verification must be submitted to NNWC_ODAA@navy.mil for Navy ODAA review.

a. Ensure implementation of personnel and non-technical security controls described in the DIP version 2.0 dated 13 Aug 09 contained in reference (v).

b. Ensure implementation of the Information Assurance Vulnerability Management program required patches/fixes per reference (b).

c. Ensure identification and currency of the Information Assurance Manager associated with this system in the DIACAP Team Roles, Member Names and Contact Information section of the SIP reference (f).

d. Ensure annual testing of your site Contingency Plan per reference (e).

e. Ensure compliance with Navy firewall configuration guidance, as defined by reference (l).

f. Ensure use of only those legacy applications that have been approved by the Functional Area Manager and accredited by the Navy ODAA.

g. Ensure compliance with requirements for proper protection of data and systems, as defined by reference (h).

h. Ensure implementation of automated enterprise-wide vulnerability scanning, security patch remediation and compliance reporting tools on Navy NIPRNET and SIPRNET assets, as directed by reference (i).

i. Per reference (m), ensure all unclassified DoD data at rest that has not been cleared for public release and is stored on mobile computing devices or removable storage media is treated as sensitive data and encrypted using DoD approved encryption technology.

j. Reference (o) expanded the requirement to complete and submit a PIA (DoD Form 2930 Nov 2008) for all DON systems whether or not the system collects, maintains or disseminates Personally Identifiable Information (PII). IT systems with no PII will submit Section 1 of the PIA form, obtain local signatures and send to DON CIO. IT systems with PII must complete Sections 1 through 4 and submit to DON CIO for approval. Reference (o) contains guidance and procedures to submit an approved PIA or a Plan of Action and Milestones (POA&M) in lieu of an approved PIA as part of the system C&A package. Questions regarding DON PIA guidance and reporting should be submitted to the DON CIO Web site: http://www.doncio.navy.mil.

k. Per reference (r), all current and new legacy systems shall be processed through the CARS case process. Upon completion of the CARS case study process you are required to submit updated C&A documentation through the Navy C&A process for review and continued authorization to operate. Submit any Excepted Network waiver received as a result of the CARS case study directly to the NNWC ODAA.

7. Reference (n) identifies DON goals to maintain 100% ATO or Interim ATO accreditation status of all systems requiring certification and accreditation, and maintain 100% compliance with FISMA required annual security reviews, annual testing of security controls, and annual evaluation of contingency plans. Each system must maintain compliance with required annual reviews, tests, and evaluations within the 12 month period of the last review cycle performed. You are required to take action to achieve DON FISMA accreditation and annual systems test, evaluation and review goals or be subject to DON non-compliance actions.

8. Consent to Monitor - In accordance with the requirements of reference (d), NAVNETWARCOM acknowledges that Defense Information Systems Agency (DISA) will conduct periodic monitoring of Navy networks. NAVNETWARCOM acknowledges and consents to DISA conducted assessments to include periodic, unannounced vulnerability assessments on connected host systems to determine effective security features and enhance IA posture.

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE
UNCLASSIFIED COMMON ACCESS CARD (CAC) PIN RESET (CPR)
WORKSTATION VERSION 2.1 ON ALL NAVY NETWORKS (FY09J0041)
DADMS 49101

9. POC: Ms. Marianne Chalut, Joint Enterprise Security Lead or Mr. Brad Martin, CTR, (757) 417-6719 ext. 0, Email: NNWC_ODAA@navy.mil.

RICHARD VOTER
By direction

Copy to:
IATS Ref # 11288
CNIC CIO Washington DC